

И.А. Шермет, академик РАН,
доктор технических наук, профессор

АННОТАЦИЯ К ТЕМАТИЧЕСКОМУ БЛОКУ

Любая социотехническая система (СТС) представляет собой совокупность трёх компонентов: социума; технологической базы, которая включает устройства и комплексы, обеспечивающие жизнедеятельность социума; и ресурсной базы, содержащей ресурсы, необходимые социуму и технологической базе для функционирования. В этом контексте целесообразно различать ресурсно-технологическую устойчивость, ресурсно-технологическую независимость и интеллектуальную независимость СТС.

Ресурсно-технологическая устойчивость СТС — её способность обеспечить себя ресурсами в ассортименте и объёмах, необходимых для существования и развития социума, в условиях деструктивных внешних воздействий со стороны враждебных систем и/или окружающей среды.

Ресурсно-технологическая независимость СТС — её способность создавать и эксплуатировать объекты техносферы, необходимые для обеспечения её ресурсно-технологической устойчивости, в условиях её частичной либо полной изоляции от содействия дружественных внешних систем.

Интеллектуальная независимость СТС — её способность самостоятельно определять и решать задачи, критически важные для обеспечения её ресурсно-технологической независимости.

Цифровой суверенитет СТС можно рассматривать как сегмент её ресурсно-технологической независимости, охватывающий её информационную инфраструктуру (технические и программные средства, обеспечивающие получение, обработку, накопление, передачу и отображение ин-

формации) и информационные ресурсы. При этом в условиях повсеместной цифровизации информационная инфраструктура естественным образом стала ядром техносферы и основой функционирования всех остальных критических инфраструктур — энергетической, транспортной, производственной, банковско-финансовой, агропромышленной и других. Поэтому цифровой суверенитет в настоящее время — это основа ресурсно-технологической независимости государства в целом. С другой стороны, распространение во всех перечисленных сферах моделей, технологий и средств искусственного интеллекта (ИИ), во многих случаях зарубежного происхождения, сделало крайне актуальными исследования, направленные на оценку степени доверия к результатам его применения. Подобные исследования подтверждают то обстоятельство, что для обеспечения реального цифрового суверенитета социотехническая система должна обладать интеллектуальной независимостью, то есть, в конечном итоге, интеллектуальным потенциалом, достаточным для определения и решения важнейших задач обеспечения её ресурсно-технологической независимости.

Настоящий номер журнала посвящён рассмотрению различных аспектов цифрового суверенитета нашей страны в условиях массового применения искусственного интеллекта в банковско-финансовой, агропромышленной и медицинской сферах, а также на объектах телекоммуникационной и энергетической инфраструктур.

В статье Л.В. Массель и А.Г. Массель предлагается методология научного обо-

снования стратегических решений по цифровой трансформации энергетики на основе ситуационного управления и цифровых двойников. Разработанная авторами архитектура мульти-агентной интеллектуальной среды обеспечивает взаимодействие цифровых двойников объектов энергетики на уровне конкретных систем и энергетической инфраструктуры в целом.

Статья А.А. Карпука и П.А. Кохно посвящена вопросам оценки качества телекоммуникационной инфраструктуры в части сотовой связи. При этом показатели качества разделены по зонам ответственности между оператором и пользователем услуг связи, что позволяет достичь компромисса между обеспечением качества услуг связи и затратами на это обеспечение.

В статье И.И. Михайленко, О.Д. Мещерякова и А.И. Литвинова рассматриваются принципы построения основанных на машинном обучении по видеоданным бесконтактных систем наблюдения за поведением животных. Авторы развивают биометрию животных путём применения нейронных сетей для решения задач регистрации, уникальной идентификации и верификации крупного рогатого скота.

В статье А.Г. Лобанова, М.В. Алиева, С.Г. Чефранова и М.Ф. Алиевой рассматриваются вопросы цифровой трансформации в растениеводстве и создания информационной инфраструктуры для комплексной обработки потоков цифровых данных с полей. Это, в свою очередь, обеспечивает переход к «сквозным» моделям селекционно-семеноводческих процессов и к интегрированному геномно-экологическому прогнозированию посредством применения методов искусственного интеллекта.

Статья В.А. Белова, Б.А. Кобринского и А.А. Акимовой содержит описание подхода и основных результатов применения методов искусственного интеллекта для оценки контролируемых факторов риска развития хронического тонзиллита и их объективной характеристики с учётом возможной неопределённости. Авторами сформировано поле знаний риск-факторов

этого заболевания, что необходимо для создания базы знаний интеллектуальной рекомендательной системы в этой области здравоохранения.

В статье О.А. Бубнова исследуется влияние уязвимостей систем искусственного интеллекта на обеспечение цифрового суверенитета Российской Федерации при их эксплуатации на объектах критической информационной инфраструктуры и в финансовом секторе. Показано, что неконтролируемое использование зарубежных моделей и средств ИИ, отсутствие стандартизированных процедур валидации моделей и недостаточная проработка вопросов кибербезопасности на всех этапах жизненного цикла ИИ создают прямые угрозы национальной безопасности в целом.

В статье С.В. Лебеда подробно анализируются различные аспекты кибербезопасности банковской инфраструктуры России в условиях роста интенсивности и расширения спектра кибератак на неё со стороны организованных сообществ киберпреступников и спецслужб враждебных и недружественных стран.

Статья А.А. Игониной посвящена детальному рассмотрению современного состояния архитектуры распределённых реестров (блокчейн), которая может использоваться в целом ряде приложений в рамках обеспечения цифрового суверенитета, и описанию предлагаемого нового подхода к реализации функций криптографического обеспечения указанной архитектуры на основе доверенных SIM-карт.

Статья Е.В. Самоходкина и А.А. Самоходкиной посвящена исследованию доверия к системам искусственного интеллекта в финансовом секторе как необходимого условия цифрового суверенитета. Показано, что доверие не сводится ни к пользовательской лояльности, ни к технической эффективности алгоритма; оно возникает на пересечении объяснимости, подотчётности, управления модельным риском, контроля над данными и инфраструктурной автономии. Обосновано, что в условиях повсеместного использования моделей

и средств ИИ зарубежного происхождения, характеризующихся непрозрачностью, доверие к ним приобретает суррогатный характер и не способствует укреплению цифрового суверенитета.

В статье А.А. Егорова и М.А. Егоровой предложена и исследована динамическая модель распространения информации в социуме. Представлены результаты теоретического анализа и компьютерного моделирования, демонстрирующие особенности поведения социума при вариации управляющих параметров. Анализ полученных результатов позволил установить области изменения параметров, при которых происходит переход от стационарного к периодическому и затем к хаотическому поведению, а впоследствии — обратный переход от хаотического к стационарному или периодическому поведению. Обращено внимание на воз-

росшую роль Интернета как глобальной инфраструктуры для реализации управляющих информационно-психологических воздействий на индивидуальное, групповое и массовое сознание.

Статья И.А. Шермета посвящена анализу больших языковых моделей (LLM) и их влияния на интеллектуальный потенциал человечества, а значит, нашей страны. Показывается, что повсеместное распространение LLM-чат-ботов и их систематическое использование, в особенности в образовательном цикле, влекут за собой риски массовой интеллектуальной деградации и утраты когнитивных способностей.

Статьи, вошедшие в номер, раскрывают различные направления и проблемы обеспечения цифрового суверенитета и могут служить основой для развёртывания и углубления дальнейших исследований по обозначенным направлениям.

I.A. Sheremet, Academician of the Russian Academy of Sciences, Doctor of Technical Sciences, Professor

ABSTRACT OF THE THEMED SECTION

Any sociotechnical system (STS) consists of three components: society; a technological base, which includes devices and complexes that support the functioning of society; and a resource base, which contains the resources required by society and the technological base for their operation. In this context, it is appropriate to distinguish between the resource-technological resilience, resource-technological independence, and intellectual independence of an STS.

The resource-technological resilience of an STS is its ability to provide itself with resources in the range and volumes necessary for the existence and development of society under destructive external impacts from hostile systems and/or the environment.

The resource-technological independence of an STS is its ability to create and operate technosphere facilities necessary to ensure its resource-technological resilience under conditions of partial or complete isolation from assistance by friendly external systems.

The intellectual independence of an STS is its ability to independently identify and solve tasks that are critically important for ensuring its resource-technological independence.

The digital sovereignty of an STS may be regarded as a segment of its resource-technological independence that covers its information infrastructure, including the hardware and software that provide for the acquisition, processing, accumulation, transmission, and display of information, as well as its informa-

tion resources. Under conditions of pervasive digitalization, information infrastructure has naturally become the core of the technosphere and the basis for the functioning of all other critical infrastructures, including energy, transport, manufacturing, banking and finance, agriculture and industry, and others. Therefore, digital sovereignty today is the foundation of the resource-technological independence of the state as a whole. On the other hand, the spread of artificial intelligence (AI) models, technologies, and tools, in many cases of foreign origin, across all the above areas has made research aimed at assessing the degree of trust in the results of their application extremely important. Such studies confirm that, in order to ensure genuine digital sovereignty, a sociotechnical system must possess intellectual independence; that is, ultimately, it must have intellectual potential sufficient to identify and solve the most important tasks involved in ensuring its resource-technological independence.

This issue of the journal is devoted to various aspects of our country's digital sovereignty under conditions of the large-scale application of artificial intelligence in the banking and financial, agricultural and industrial, and medical sectors, as well as at facilities of telecommunications and energy infrastructure.

The article by L.V. Massel and A.G. Massel proposes a methodology for the scientific substantiation of strategic decisions on the digital transformation of the energy sector based on situational management and digital twins. The multi-agent intelligent environment architecture developed by the authors ensures the interaction of digital twins of energy facilities both at the level of specific systems and at the level of the energy infrastructure as a whole.

The article by A.A. Karpuk and P.A. Kokhno addresses the assessment of the quality of telecommunications infrastructure with respect to cellular communications. In this context, quality indicators are divided between the areas of responsibility of the communications service operator and the user, which makes it possible to achieve a

compromise between ensuring the quality of communications services and the costs required to provide it.

The article by I.I. Mikhaylenko, O.D. Meshcheryakova, and A.I. Litvinov examines the principles of designing contactless systems for observing animal behavior based on machine learning from video data. The authors develop animal biometrics by applying neural networks to the tasks of registration, unique identification, and verification of cattle.

The article by A.G. Lobanov, M.V. Alieva, S.G. Chefranov, and M.F. Alieva considers issues of digital transformation in crop production and the creation of information infrastructure for the integrated processing of digital data flows from fields. This, in turn, enables a transition to end-to-end models of breeding and seed-production processes and to integrated genomic-environmental forecasting through the use of artificial intelligence methods.

The article by V.A. Belov, B.A. Kobrinsky, and A.A. Akimova describes an approach to, and the main results of, applying artificial intelligence methods to assess controllable risk factors for chronic tonsillitis and to provide their objective characterization while taking possible uncertainty into account. The authors form a knowledge field of risk factors for this disease, which is necessary for creating the knowledge base of an intelligent recommender system in this area of healthcare.

The article by O.A. Bubnov examines the influence of vulnerabilities in artificial intelligence systems on ensuring the digital sovereignty of the Russian Federation when such systems are operated at critical information infrastructure facilities and in the financial sector. It is shown that the uncontrolled use of foreign AI models and tools, the absence of standardized model validation procedures, and insufficient elaboration of cybersecurity issues at all stages of the AI life cycle create direct threats to national security as a whole.

The article by S.V. Lebed provides a detailed analysis of various aspects of cybersecurity in Russia's banking infrastructure amid increasing intensity and a broadening spectrum of cyberattacks carried out against

it by organized cybercriminal communities and the special services of hostile and unfriendly countries.

The article by A.A. Igonin is devoted to a detailed consideration of the current state of distributed ledger architecture (blockchain), which can be used in a wide range of applications related to ensuring digital sovereignty, and to a description of a proposed new approach to implementing cryptographic support functions for this architecture on the basis of trusted SIM cards.

The article by E.V. Samokhodkin and A.A. Samokhodkina is devoted to the study of trust in artificial intelligence systems in the financial sector as a necessary condition for digital sovereignty. It is shown that trust is reducible neither to user loyalty nor to the technical efficiency of an algorithm; rather, it emerges at the intersection of explainability, accountability, model risk management, control over data, and infrastructural autonomy. It is substantiated that, under conditions of the pervasive use of AI models and tools of foreign origin characterized by opacity, trust in them becomes surrogate in nature and does not contribute to strengthening digital sovereignty.

The article by A.A. Egorov and M.A. Egorova proposes and studies a dynamic model

of information dissemination in society. The results of theoretical analysis and computer simulation are presented, demonstrating the features of societal behavior as control parameters vary. Analysis of the results obtained made it possible to identify parameter ranges in which a transition occurs from stationary behavior to periodic and then chaotic behavior, followed subsequently by a reverse transition from chaotic behavior to stationary or periodic behavior. Attention is drawn to the growing role of the Internet as a global infrastructure for implementing controlling informational and psychological influences on individual, group, and mass consciousness.

The article by I.A. Sheremet is devoted to an analysis of large language models (LLMs) and their influence on the intellectual potential of humanity and, consequently, of our country. It is shown that the widespread dissemination of LLM chatbots and their systematic use, especially in the educational cycle, entail risks of mass intellectual degradation and loss of cognitive abilities.

The articles included in this issue reveal various directions and problems in ensuring digital sovereignty and may serve as a basis for expanding and deepening further research in the areas indicated.